Lab 280

Morris & Opazo

aws re/start

# Malware de firewall

# INTRODUCCIÓN

Las amenazas de malware pueden estar presentes, y las organizaciones pueden usar varias técnicas y servicios para mitigar estas amenazas (por ejemplo, firewalls, software antivirus y prácticas recomendadas de control de usuarios). Este laboratorio se enfoca en técnicas de contramedidas usando un firewall.

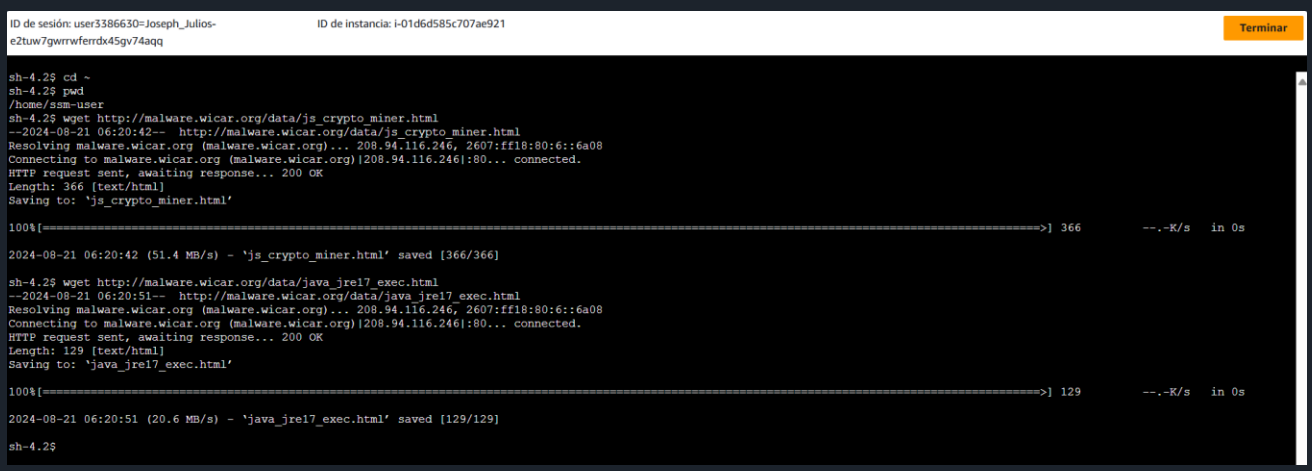
# OBJETIVOS

- Actualizar un firewall de red de AWS
- Crear un grupo de reglas de firewall
- Verificar y probar que el acceso a los sitios maliciosos esté bloqueado

# TAREA 1

En esta tarea, inicia sesión en la instancia TestInstance de EC2 que se preconfiguró durante la preparación del laboratorio. Desde ahí, emite un comando wget a los archivos del actor malicioso que el equipo de TI le proporcionó para confirmar la accesibilidad.

- Desde la página de la consola de Vocareum, seleccione el botón de detalles de AWS.
- Junto a TestInstanceURL, hay un enlace. Copie y pegue el enlace en un nuevo laboratorio en su navegador web.
- Cambiar directorios y ver el directorio de trabajo actual.
- En este entorno de laboratorio protegido, ingrese el código y presione Intro para descargar parte del malware.
- En este entorno de laboratorio protegido, ingrese el código y presione Intro para descargar el resto del malware.



- Ver los archivos descargados.

ID de sesión: user3386630=Joseph_Julios-e2tuw7gwrrwferrdx45gv74aqq

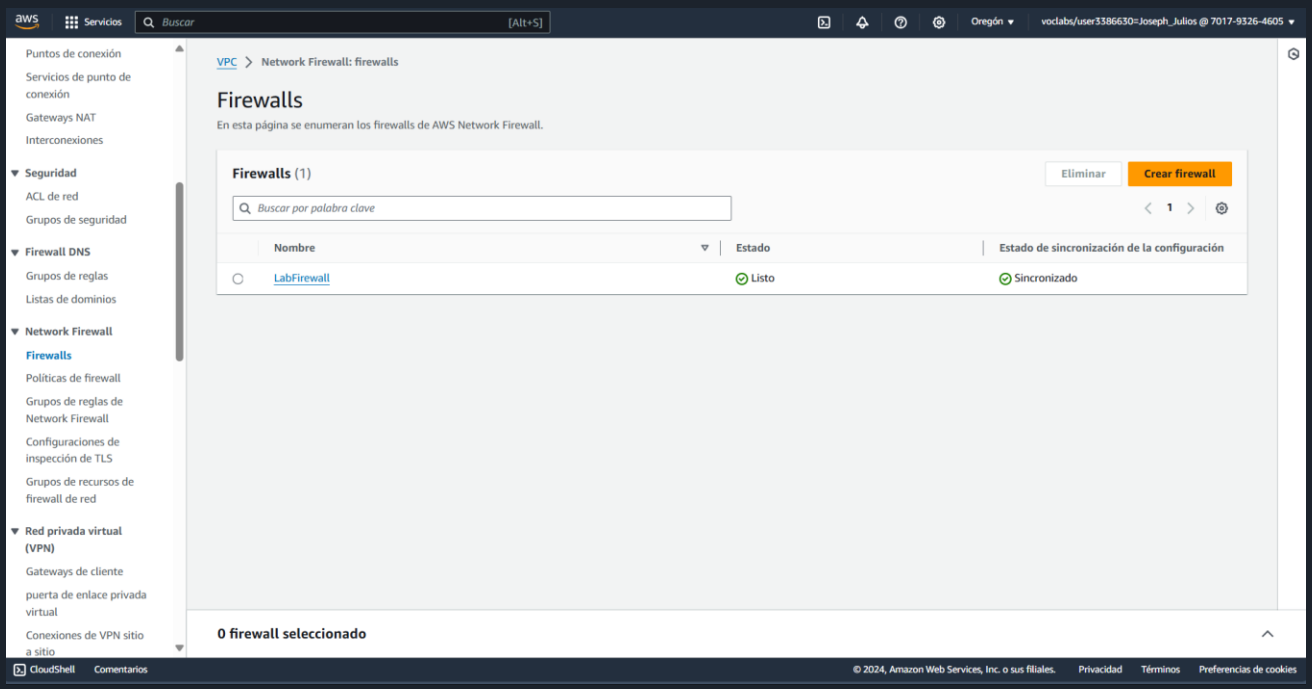
ID de instancia: i-01d6d585c707ae921

```
sh-4.2$ ls
java_jre17_exec.html  js_crypto_miner.html
sh-4.2$
```

# TAREA 2

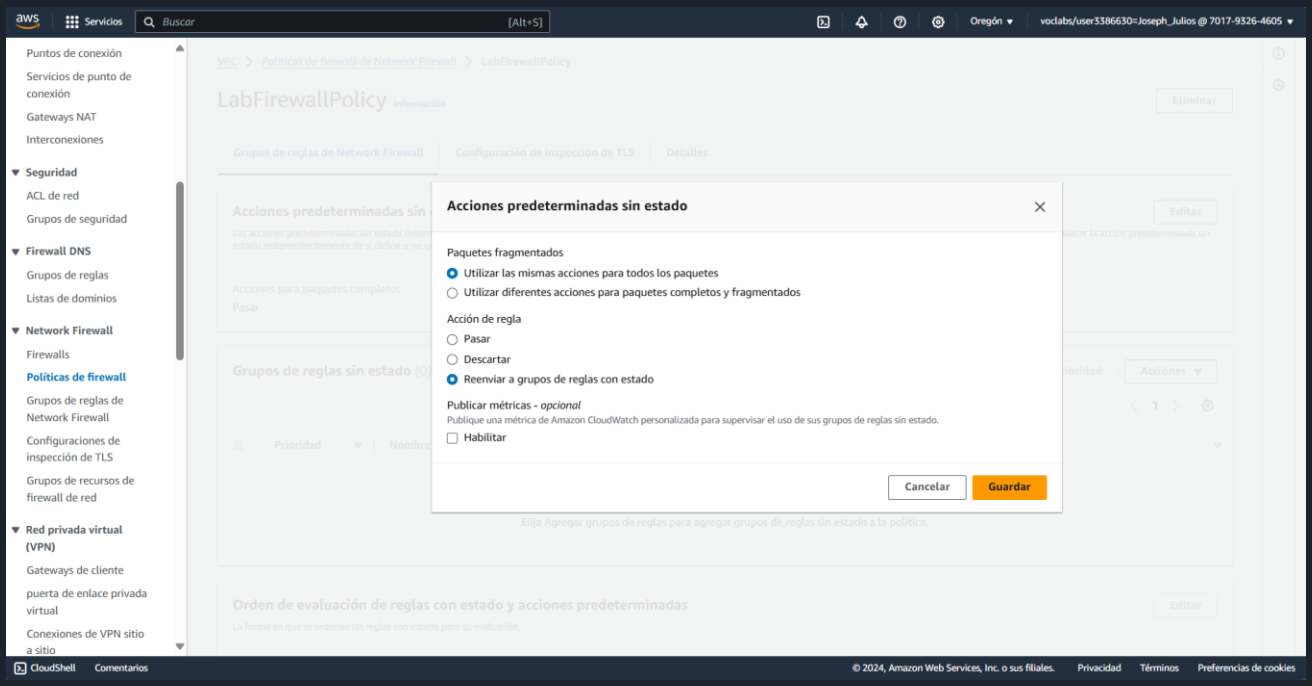
En esta tarea, inspeccionará el firewall de AWS Network Firewall que se configuró durante la preparación del laboratorio. Actualizar este firewall es la prioridad principal que le asignó AnyCompany como el nuevo ingeniero de seguridad.

- En la consola de administración de AWS, ingrese VPC en la barra de búsqueda y luego seleccione VPC.
- En el panel de navegación izquierdo, en NETWORK FIREWALL, seleccione Firewalls




- Seleccione LabFirewall y lea los tres pasos en la sección Overview.

- En el Paso 2: Configurar la política de firewall, seleccione el enlace de LabFirewallPolicy para abrir la política asociada.
- En la sección Stateless default actions, seleccione Edit.
- Para Stateless default actions (Acciones predeterminadas sin estado), configure las siguientes opciones.

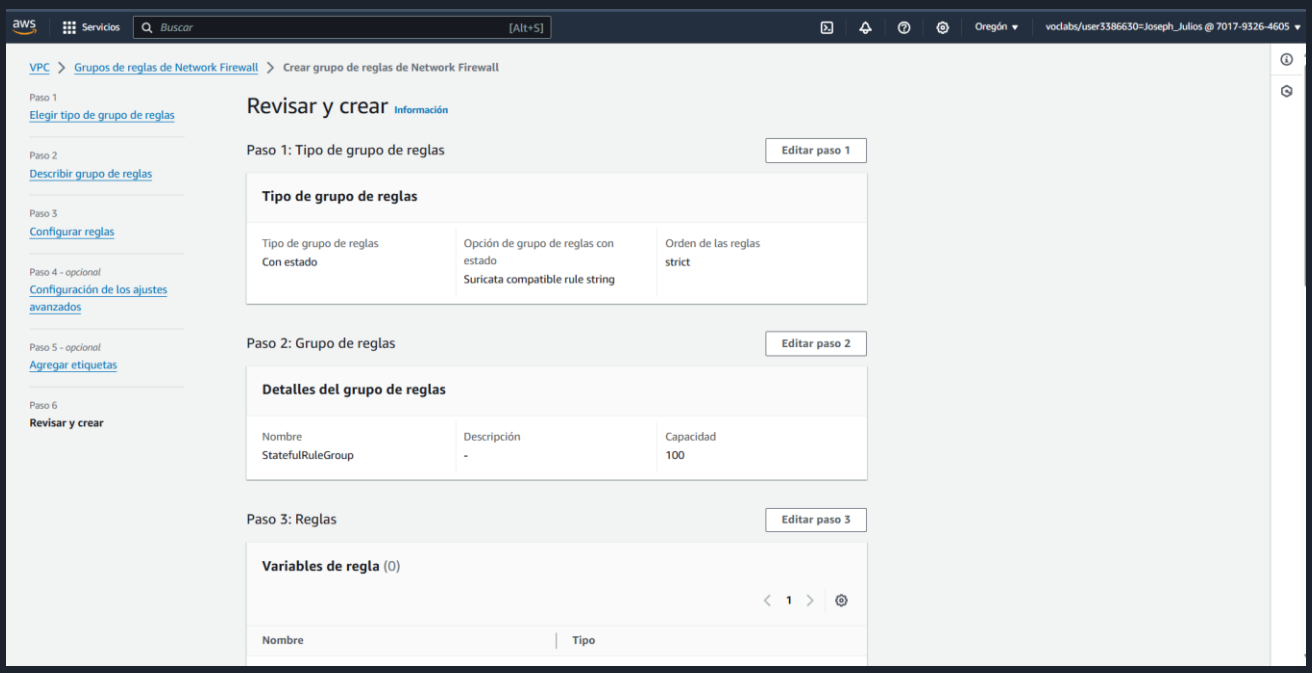



- Seleccione Save (Guardar).

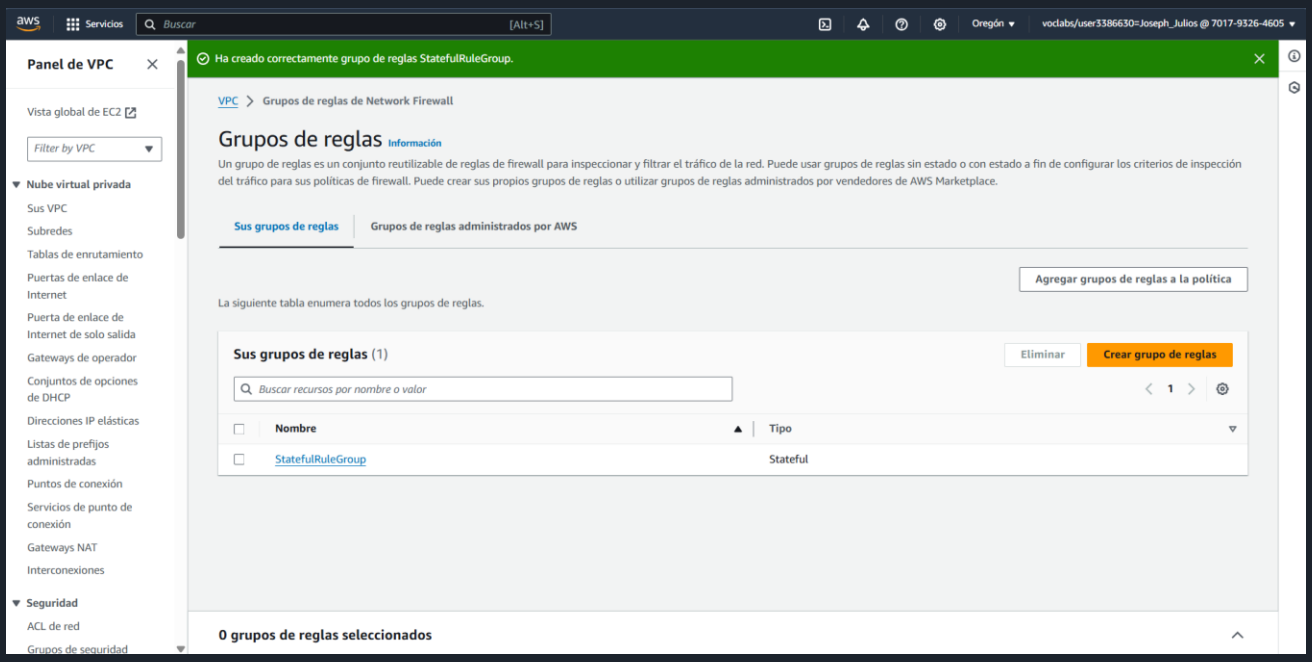
# TAREA 3

En esta tarea, creará un grupo de reglas de firewall de red con reglas que bloquean el acceso a las URL maliciosas. Luego adjuntará esta regla a su política de firewall.

- En el panel de navegación izquierdo, en NETWORK FIREWALL, seleccione Network Firewall Rule Groups.
- Seleccione Create Network Firewall rule group.
- En la sección Create Network Firewall rule group (Crear grupo de reglas de firewall de red), configure las opciones de Rule group type y Stateful rule group.
- En la sección Suricata compatible IPS rules, ingrese el código en el cuadro de texto.



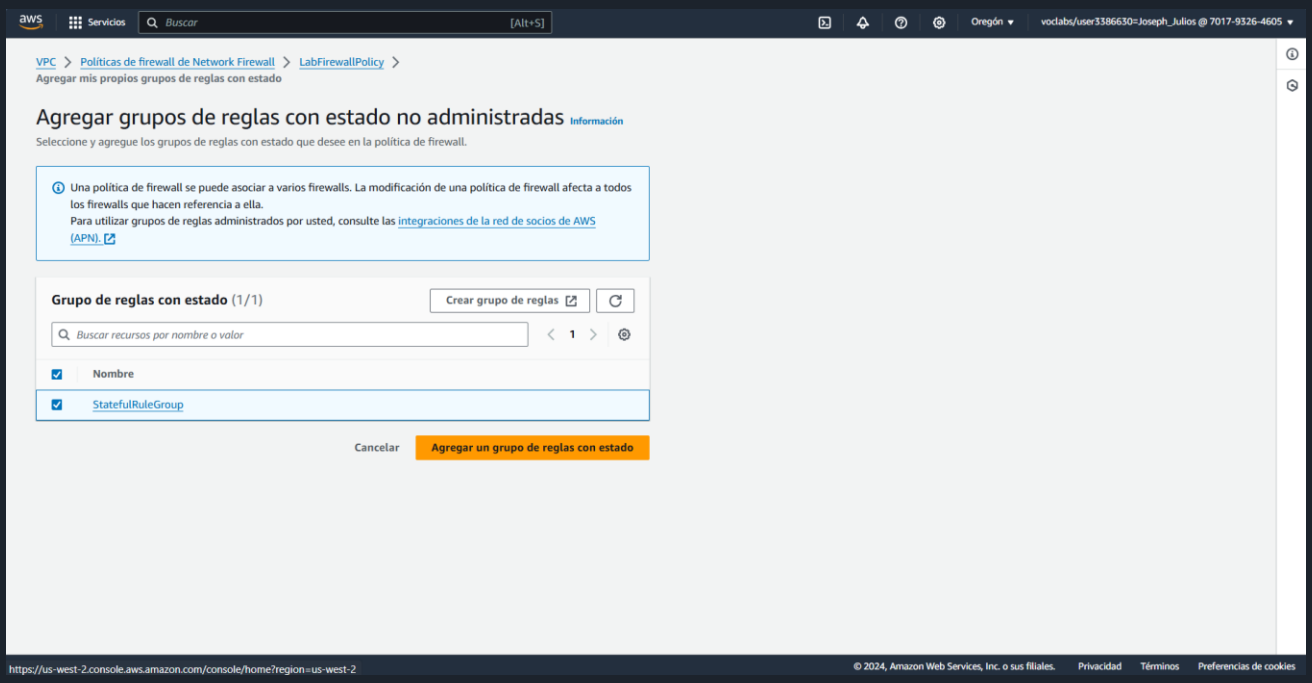
- Seleccione Create stateful rule group.



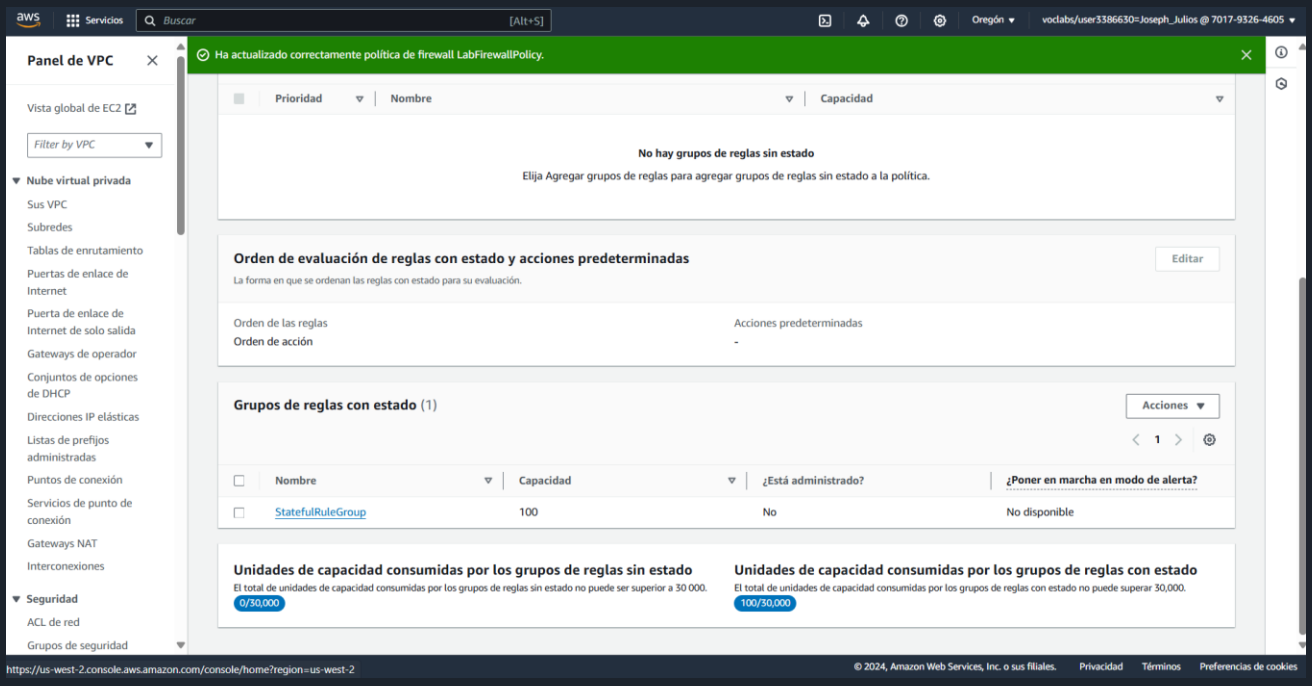
# TAREA 4

En esta tarea, adjuntará el grupo de reglas de firewall de red que creó al firewall de red.

- En el panel de navegación izquierdo, en NETWORK FIREWALL, seleccione Firewalls.
- Seleccione LabFirewall.
- En Step 2, seleccione la lista desplegable Add rule groups y luego seleccione Add from existing stateful rule groups.
- Seleccione la casilla para StatefulRuleGroup y luego seleccione Add stateful rule group.



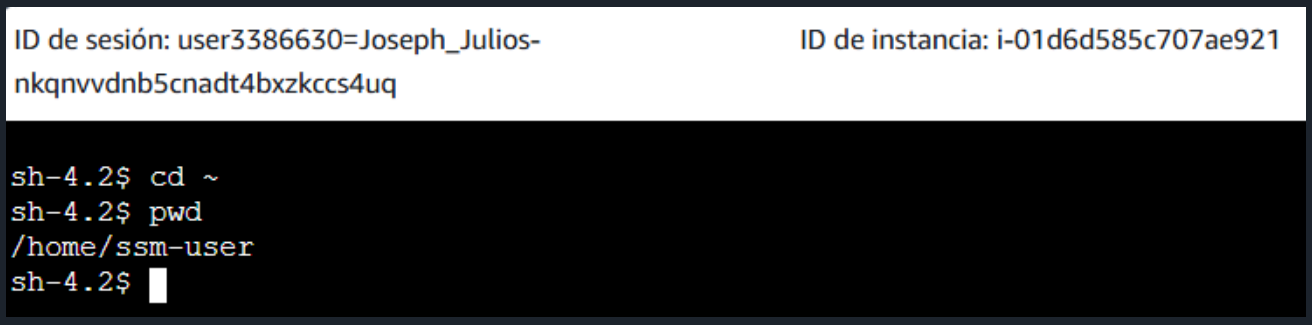
- Desplácese hasta la sección Stateful rule groups para ver el grupo de reglas que se agregó correctamente.



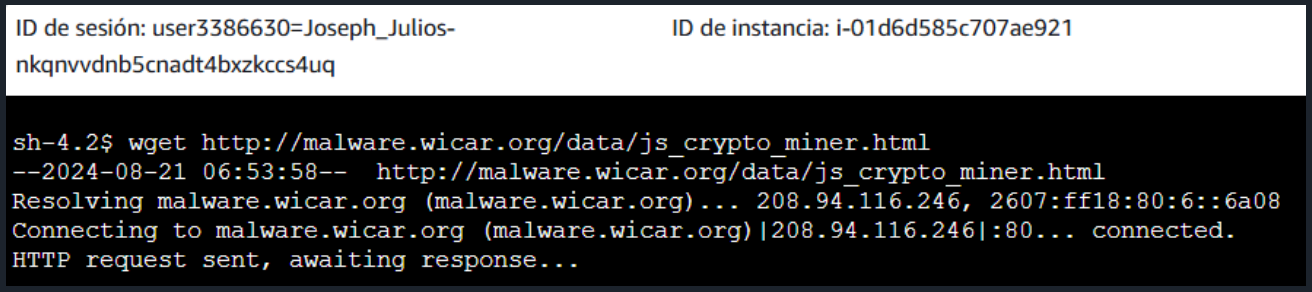
# TAREA 5

En esta tarea, volverá a iniciar sesión en TestInstance para probar que el firewall de red bloquee correctamente los intentos de acceder a los archivos del sitio web malicioso.

- En la consola de administración de AWS, ingrese EC2 en la barra de búsqueda y luego seleccione EC2.
- En el panel de navegación izquierdo, elija Instances.
- Seleccione la casilla junto a TestInstance, y luego seleccione Connect.
- Cambiar directorios y ver el directorio de trabajo actual.




- Para intentar acceder al primer archivo malicioso, ejecute el siguiente comando wget.



- Presione Ctrl+c para detener el comando.
- Para probar las otras URL maliciosas, ejecute el siguiente comando.

ID de sesión: user3386630=Joseph_Julios-nkqnvvdnb5cnadt4bxzkccs4uq ID de instancia: i-01d6d585c707ae921

```
sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2024-08-21 06:55:06--  http://malware.wicar.org/data/java_jre17_exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:ff18:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response...
```

- A continuación, para eliminar los archivos de malware de prueba, ejecute el siguiente comando.
- Confirmar que los archivos se eliminaron.

ID de sesión: user3386630=Joseph_Julios-nkqnvvdnb5cnadt4bxzkccs4uq ID de instancia: i-01d6d585c707ae921

```
sh-4.2$ rm java_jre17_exec.html js_crypto_miner.html
sh-4.2$ ls
sh-4.2$
```